Évaluation automatique des méthodes de tatouage

Automatic evaluation of watermarking schemes

par F. RAYNAL[1], F.A.P PETITCOLAS[2], C. FONTAINE[3]

[1] INRIA Rocquencourt, frederic.raynal@inria.fr
[2] Microsoft Research, fabienpe@microsoft.com
[3] USTL-LIFL, caroline.fontaine@lifl.fr

résumé et mots clés

Les méthodes de tatouage sont de plus en plus nombreuses. Néanmoins, il est difficile de les comparer et de trouver celle adaptée à ses besoins dans la mesure où les tests présentés sont très souvent différents. En effet, tant les média employés que les transformations qu'ils subissent changent d'une étude à l'autre.
Dans cet article, nous présentons `StirMark Benchmark 4`, un outil d'évaluation automatique pour les schémas de tatouage. Il est développé en C++, selon un modèle orienté objets, ce qui nous a permis de l'adapter à la fois aux images et aux fichiers audios.
Les algorithmes de tatouage étant tous dissemblables, nous utilisons des *profils* qui définissent les tests à appliquer aux méthodes, selon les paramètres dont elles se servent et les objectifs poursuivis. Nous proposons également des niveaux d'assurance sur les critères habituels (perceptibilité, robustesse et capacité) afin de faciliter la lisibilité des performances obtenues par les schémas. Nous présentons aussi de nouveaux tests (audio, espace des-clés, fausses alarmes, marquage multiple).

Tatouage, évaluation, protocole expérimental.

abstract and key words

Many watermarking schemes are now well defined, but it is still very difficult to compare them and thus find the one which fits our needs. Since both media and attacks used for evaluation are different in each article, it is almost impossible to compare the schemes.In this article, we introduce `StirMark Benchmark 4`, a new automatic tool to evaluate watermarking schemes. It is written in C++, according to an object oriented model, which allows us towork on images and audio files.There are many different applications for watermarking, so we use *profiles* to define tests to apply according to the requested parameters of the method, and its purposes. We also propose different levels of quality on usual criteria (perceptibility, robustness and capacity) to increase the legibility of the performances obtained by the schemes. We also introduce new tests (audio, key space, falsealarms, multiple watermarking).

Watermarking, evaluation, experiment protocol.

1. introduction

Le domaine du tatouage numérique connaît un essor important depuis quelques années et le besoin de solutions efficaces se fait d'autant plus sentir que les outils numériques deviennent de plus en plus accessibles. Les techniques de tatouage se multiplient, mais aucune ne parvient encore à s'imposer. En effet, les utilisateurs potentiels de schémas de tatouage ne savent à quel algorithme se fier car il n'existe toujours pas de programme permettant une évaluation fine bien que les premières tentatives apparurent dès 1998 [PAK98]. Ce manque de référence provoque une grande confusion qui empêche tous les acteurs concernés (ayants-droit de ces média, fabricants de matériels ou éditeurs de logiciels) de sélectionner une solution appropriée à leurs besoins : fonder une politique de protection à long terme sur des schémas peu testés ne ressemble pas à une idée pertinente.

Après avoir mis au point le protocole expérimental le modèle générique des tests, indépendant du médium considéré, nous avons commencé à l'adapter aux images. Par la suite, M. Steinebach[1] et J. Dittman, de l'Université de Darmstadt en Allemagne, nous ont rejoints pour traiter la partie audio à partir du travail déjà réalisé pour les images ([PSR+01, SPR+01).

Deux autres projets similaires existent. Tout d'abord, le projet Européen Certimark, lancé en Mai 2001 sous la direction de C. Rollin (Société des Auteurs et Compositeurs Dramatiques – SACD), et regroupant 15 partenaires, travaille principalement dans deux directions :

1. élaboration et développement d'un outil d'évaluation pour le tatouage ;

– outil d'évaluation complet pour les images et les vidéos ;

– création de nouvelles attaques, élaboration de nouveaux tests pour tout type de paramètres, définition d'une nouvelle mesure qualitative pour les images.

2. recherche sur des algorithmes de tatouage :

– élaboration de méthodes de tatouage en profitant des compétences variées de tous les participants ;

– évaluations des techniques les plus efficaces pour une exploitation commerciale future.

On trouve également le projet `checkmark` lancé par S. Pereira et supervisé par T. Pun ([PVM+01, VPP+01]). Ce programme, développé pour `Matlab 6`, contient de nombreux tests (compression par ondelettes, attaque par recopie par exemple) et s'appuie sur une métrique plus performante que le PSNR : la métrique de Watson ([MEC98]). Celle-ci prend mieux en compte la luminance et le contraste d'une image que le PSNR.

Ces projets sont complémentaires, en particulier par le grand nombre de tests différents qu'ils proposent. Par ailleurs, ils offrent la possibilité de travailler dans des environnements différents, tant par le langage utilisé (`Matlab` ou `C++`) que par le support des média (images uniquement, ou bien également des sons ou vidéos).

Nous présentons tout d'abord les conditions générales indispensables à l'utilisation d'un logiciel d'évaluation. Ensuite, nous introduisons l'architecture globale du système. Enfin, une dernière partie est consacrée à l'évaluation elle-même, détaillant les niveaux d'assurances de différents critères ainsi que de nouveaux tests.

2. pré-requis pour un outil d'évaluation

Le tatouage numérique reste un champ d'investigations où les évaluations précises sont encore peu répandues. D'une part, peu d'organismes ont déjà fourni un cahier des charges complet, détaillant précisément les spécifications attendues qui permettraient de valider, ou au moins de tester, les méthodes proposées ([Int97],[Euro00]). D'autre part, les équipes de recherche ou les sociétés ne publient que très rarement les résultats des tests intensifs menés sur leurs solutions [Bra98].

De plus en plus d'attaques sont recensées contre les schémas de tatouage ([PAK98, LvD98, SG00, KVH00, HSG00]). Cela illustre bien la nécessité d'accroître les performances des algorithmes de tatouage de sorte que les nouveaux standards multimédia puissent s'appliquer, entre autre, à la protection des droits d'auteur.

Les tests réalisés dans les diverses publications ne présentent que des résultats partiels, obtenus à partir d'un ensemble restreint de média et d'attaques, en appliquant un protocole expérimental personnel. Ce point, déjà présenté dans [KP99], démontre l'impossibilité de comparer les solutions élaborées les unes par rapport aux autres, à moins de reprogrammer soi-même les algorithmes.

Cependant, cela conduirait très certainement à des implantations informatiques différentes, probablement moins performantes que celles des auteurs initiaux puisque les détails des algorithmes, très importants pour une comparaison impartiale, sont rarement publiés. Ce manque d'étalonnage laisse à penser que le besoin d'une référence commune dans l'évaluation des schémas de tatouage est urgent.

À l'aide de cette référence commune et précise, les chercheurs et industriels du secteur n'auront alors qu'à fournir un tableau de résultats qui reflétera les performances du schéma proposé. Les utilisateurs finaux pourront vérifier alors si leurs attentes sont satisfaites. De leur côté, les chercheurs verront les conséquences d'un changement dans une méthode, et seront à même d'en évaluer la pertinence. Ce protocole expérimental facilitera les développements initiaux d'une solution en identifiant rapidement ses forces et faiblesses. Enfin, les industriels connaîtront le degré de confiance à accorder àun schéma de tatouage.

Nous n'abordons ici que l'évaluation des méthodes de tatouage elles-mêmes. Cependant, le cadre d'utilisation de ces algo-

rithmes dépasse la simple volonté de dissimuler une marque dans un médium. Les systèmes qui les emploient poursuivent des objectifs différents (commerce d'images, de vidéo ou de fichiers sons par exemple) et s'appuient aussi sur d'autres techniques, bien souvent liées à la cryptographie. Dans ce contexte, un protocole, une configuration ou encore un générateur aléatoire peuvent tout autant se révéler vulnérables.

2.1. nécessité d'un tiers de confiance

Les performances d'une méthode de tatouage doivent être évaluées et rendues publiques afin que les utilisateurs sachent quelle approche employer. Plusieurs solutions sont envisageables pour la mise en œuvre de ces tests :

– faire confiance à qui fournit la méthode, ainsi qu'aux résultats qu'elle affiche ;

– réaliser soi-même les tests pour vérifier que la méthode répond à ses propres attentes ;

– laisser un tiers indépendant évaluer la méthode.

Seule la dernière démarche permet d'obtenir un résultat objectif, à la condition impérative que la méthodologie et les outils employés soient eux-mêmes connus de tous. Ainsi, les sources du programme seront accessibles à tous, de même que divers documents, comme celui-ci, détaillant le protocole expérimental. Cette approche permettra à chacun de reproduire aisément les tests réalisés sur la plate-forme publique.

La mise en œuvre d'un tel système soulève de nombreux problèmes. Ainsi, le concepteur d'un algorithme de tatouage doit-il envoyer son programme sous forme de sources ou d'exécutable ? Ou bien l'évaluation est-elle accomplie à distance par le biais de preuves interactives fondées sur des échanges entre le testeur et le concepteur ?

Sur ce dernier modèle, on peut imaginer l'approche suivante, inspirée des preuves à divulgation nulle de connaissance (*zero-kwnoledge proof* – [Kah96, MvOV99]). Ces protocoles mettent en scènes un vérificateur V et un prouveur P. Le but de P est de convaincre V qu'il connaît un secret sans révéler la moindre information sur celui-ci. En appliquant ce modèle à l'évaluation de schémas de tatouage, P cherche à convaincre V de la résistance de son algorithme à la transformation f :

1. V envoie à P un médium m ;

– P marque m, produisant le médium $\widetilde{m}$, qu'il renvoie à V ;

– V renvoie à P le médium $m' = f(m_b)$, où $b \in \{0, 1\}$, généré aléatoirement, est tel que $m_0 = m$ et $m_1 = \widetilde{m}$;

– P annonce s'il réussit ou non à retrouver la marque.

Si P triche, il a une chance sur deux de se faire prendre et un chance sur deux de tromper le vérificateur. Donc, au bout de n essais, la probabilité qu'il triche sans se faire prendre est $1/2^n$. Malheureusement, si ce protocole fonctionne parfaitement dans les cas d'authentification, ce n'est plus vrai pour l'évaluation. D'une part, V dispose alors du médium initial et de sa version marquée, ce qui peut lui permettre de construire des attaques en choisissant les média appropriés. D'autre part, la majorité des transformations f sont facilement inversibles, ou au moins compensables, même si P ne connaît pas f. En effet, P dispose du médium original m, du médium marqué $\widetilde{m}$ et d'un médium à tester m'. Il lui suffit simplement de comparer m' à m et $\widetilde{m}$ pour obtenir une bonne idée de f^{-1}, et ensuite rechercher la marque dans $f^{-1}(m')$. Ceci démontre, outre l'inadaptation de ce protocole expérimental, que le vérificateur doit au moins disposer du mécanisme d'insertion ou de détection/extraction.

2.2. conditions requises

Une autre difficulté qui se dresse dans l'élaboration d'un outil d'évaluation automatique des méthodes de tatouage provient de la diversité des algorithmes et des média. En effet, une même catégorie de média contient des éléments très différents les uns des autres, aussi bien au niveau du sens (un concert de musique religieuse ou de hard rock) que de la représentation (une même note jouée par divers instruments ne possède pas le même timbre). Par ailleurs, certains algorithmes sont dédiés à un type d'images ou de sons précis alors que d'autres se veulent plus généraux. La composition de notre base de média doit donc être variée.

Ainsi, chaque méthode est testée sur un sous-ensemble de média généré aléatoirement. Dans un second temps, l'utilisateur pourra également spécifier une ou plusieurs catégories de média particuliers (images médicales, satellites, de synthèse, et autres), soit au vu des résultats obtenus, soit parce que l'algorithme est dédié à ce type précis de média. De cette constatation, nous avons conclu que notre outil devait être simple et modulaire.

2.2.1. simplicité

Pour être largement accepté, ce service d'évaluation s'appuie sur une interface simple, compatible avec les bibliothèques de marquage déjà existantes. L'utilisateur fournit trois fonctions : la première pour insérer une marque, la deuxième pour la détecter et une dernière permettant de donner des informations sur la méthode utilisée (*cf.* section 3.1.). Comme nous l'avons déjà évoqué, les schémas de tatouage ne répondent pas tous aux mêmes besoins, et nous proposons donc des profils d'évaluation adaptés (ensembles de média et de tests). Ces objectifs sont résumés dans la figure 1.

Le service lui-même repose sur un simple modèle client-serveur :

le client envoie une bibliothèque compilée respectant l'interface, puis spécifie le profil d'évaluation souhaité ; un automate déclenche la batterie de tests sélectionnés,et dès qu'ils sont terminés, les résultats sont retournés au client et peuvent être rendus publics, à la demande du client.

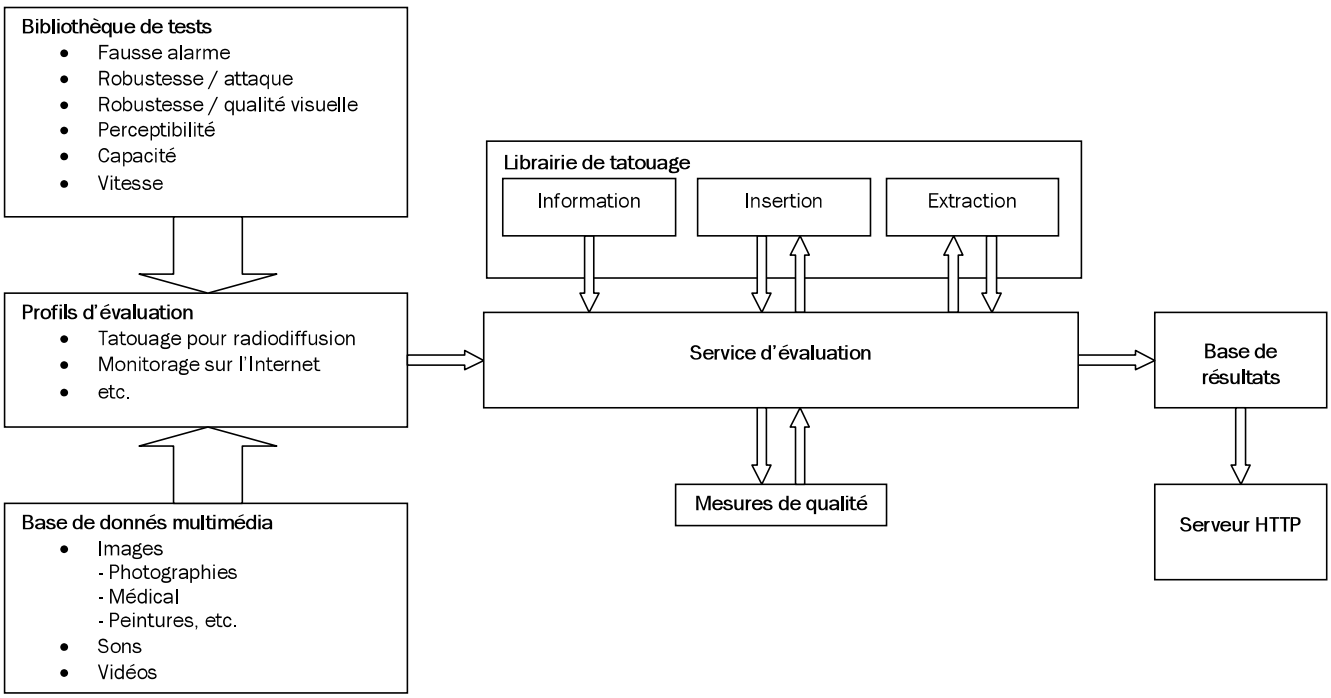

Figure 1. – Fonctionnement général de `StirMark Benchmark 4`.

2.2.2. modularité

Pour parvenir à un mécanisme pertinent d'évaluation, la première tâche consiste à identifier les différents objectifs poursuivis par les schémas de tatouage :

– *identification de signaux audiovisuels* : la marque transporte un numéro d'identification unique, type ISBN, servant de clé pour une base de données. Ceci permet d'associer à un contenu différentes informations, comme une licence. Cependant, dans certaines occasions, il vaut mieux dissimuler directement les données dans le médium plutôt que sur une base de données centrale afin d'éviter une connexion à un serveur distant ;

– *preuve de propriété* : la marque dissimulée permet à une autorité de connaître l'ayant-droit ou le créateur d'un médium ;

– *audit* : la marque contient une information utilisée pour identifier les acteurs en présence lors d'une transaction autour du médium (*i.e.* le distributeur et l'utilisateur final). Cette trace montre le transfert entre les parties. Les marques qui permettent d'identifier les utilisateurs sont couramment appelées *empreintes* ;

– *contrôle de copies* : la marque dénombre les copies effectuées, ce qui permet d'en contrôler la quantité effectuée. De telles protections sont employées pour prévenir la copie de Digital Versatile Disks (DVD) [BCL+99] ou de fichiers audio (par Sony avec le format ATRAC3) ;

– *contrôle de l'utilisation du médium* : le médium comporte en guise de marque une sorte de numéro de licence. En parallèle, un automate vérifie sur la toile que les utilisateurs sont bien valides ;

– *preuve d'altération* : certaines marques permettent de détecter les modifications subies ultérieurement par le médium ;

– *avertissement aux utilisateurs* : ce type de marque prévient l'utilisateur d'un médium de son copyright. Par exemple, lorsqu'une personne cherche à sauvegarder le médium protégé, un message d'avertissement est alors affiché.

De nombreuses autres utilisations illustrent encore la diversité des attentes. Dans ces conditions, il est indispensable que l'outil d'évaluation soit compatible avec ces applications. Cela passe par la définition de profils, répondant à chaque objectif recherché. Cette tâche délicate nécessite l'agrément de la communauté scientifique. Les profils sont proposés à titre indicatif et peuvent être affinés soit *a priori*, soit *a posteriori* au vu des résultats obtenus lors d'un précédent test.

Tester l'intégralité de tels systèmes dépasse largement le cadre de notre outil : nous ne nous intéressons ici qu'à l'aspect tatouage. De ce fait, les principaux critères à évaluer sont la perceptibilité, la fiabilité (robustesse et fausses alarmes), la capacité ou encore la rapidité. De plus amples détails sont présentés au paragraphe 4, tant sur le sens de ces termes que sur les solutionsmises en œuvre pour les quantifier. Chaque paramètre est plus ou moins corrélé aux autres. Des bibliothèques spécifiques dédiées à leur évaluation reposent sur des tests *ad hoc*, comme ceux décrits dans [KP99].

3. architecture de `StirMark Benchmark 4`

3.1. interface

Pour se servir de `StirMark Benchmark 4`, un utilisateur soumet sa méthode de tatouage sous forme de bibliothèque compilée, soit pour Windows, soit pour Linux, exportant trois fonctions.
La première, `GetSchemeInfo`, fournit des informations sur la méthode, comme sa catégorie (privé, aveugle, asymétrique), son type (I ou II), son auteur, sa version, sa date de mise en disponibilité, une description.
Les deux autres fonctions sont `Embed` et sa complémentaire `Extract`. Elles utilisent un ensemble de paramètres, certains obligatoires et d'autres optionnels selon le type de tatouage. Ils comprennent le médium original, la marque, la clé d'insertion, la *force* d'incrustation, la tolérance maximale autorisée, *etc*. Cette approche permet de conserver une compatibilité entre les différentes méthodes de tatouage.
La *force* représente un compromis entre l'imperceptibilité, la capacité et la fiabilité procurées par l'algorithme. Elle vérifie les propriétés suivantes :
– il s'agit d'un réel (`float`) compris entre 0 et 100 ;
– plus la force est élevée, plus la qualité de l'image en sortie se dégrade, mais, si tout va bien, la robustesse s'accroît d'autant ;
– une force nulle correspond àune absence de marque (PSNR tendant vers ∞) ;
– une force de 100 implique un médium marqué avec un PSNR proche de 20dB ;
– la distribution de la force doit être harmonieuse. Le PSNR espéré devrait être proportionnel à $-20\log_{10}\left(\frac{1000}{\text{force}}\right)$[1], autrement dit la force est proportionnelle à l'énergie du bruit. Le tableau 1 fournit la correspondance entre force et PSNR.

Tableau 1. – Correspondance entre force et PSNR.

force	0.1	0.5	1	10	30	50	70	80	90	100
PSNR	80	66.02	60	40	30.46	27.96	23.1	21.94	20.92	20

3.2. profils

Le support de différentes applications de tatouage est obtenu grâce à une initialisation dépendant du profil spécifié ([Pet00]). Un profil est construit autour d'un ensemble de tests, avec les paramètres appropriés. Le tableau 2 illustre ce mécanisme pour un schéma applicable à la diffusion radiophonique, et un autre correspondant à une vérification pour des images.

Tableau 2. – Exemples simplifiés de profils d'évaluation : chaque profil est composé d'un ensemble de tests avec leurs paramètres et d'une liste d'ensembles d'échantillons.

Marquage audio aveugle	**Marquage d'image**
[Test list] Test 1=Mean embedding time Test 2=Mean extraction time Test 3=Sound Low pass filter [Mean embedding time] Number of tests=100 [Mean extraction time] Number of tests=100000 [Sound Low pass filter] Cut frequency=2000 [Samples] Set 1=Radio broadcasts Set 2=Voices Set 3=Songs	[Test list] Test 1=Mean embedding time Test 2=Noise addition Test 3=Image JPEG compression [Mean embedding time] Number of tests=100000 [Noise addition] Noise start level=0.25 Noise end level=0.75 Step=0.05 [JPEG compression] Quality start=100 Quality end=75 Step=5 [Samples] Set 1=Medical pictures Set 2=Photographs

Dans un profil, l'utilisateur définit d'abord les tests auxquels doit être soumis son schéma. Ensuite, pour chaque test prévu, les paramètres sont précisés. Des paramètres par défaut sont offerts dans les classes de bases mais il est très facile pour le programmeur d'un nouveau test de spécifier les siens. Par exemple, pour la compression JPEG, on donne la qualité minimale, la qualité maximale et le pas. Enfin, il est possible de préciser des ensembles de média.

3.3. arborescence de classes

Le programme est écrit en `C++` afin de bénéficier des avantages de l'héritage et du polymorphisme de classes. Notre ambition est de fournir un outil permettant d'évaluer des schémas indistinctement pour les différents média (images, sons, vidéos). La figure 2 présente une version simplifiée de l'arborescence de classes.
`CBench` est une classe générale pour toutes les évaluations possibles. Elle initialise une liste de tests selon le profil désiré. Elle utilise la classe `CMarkingScheme` comme interface entre la bibliothèque fournie par l'utilisateur et les tests. La classe

1. Dans [BSC01], les auteurs fournissent une estimation de la déformation subie par l'image après l'insertion de la marque dans un schéma utilisant une DCT : $PSNR = 20\log_{10}255 - 10\log_{10}(\sigma_I^2 - \sigma_\mu^2) - 20\log_{10}\alpha$, où σ_I^2 représente la variance de la luminance de l'image I, σ_μ^2 la variance de la moyenne de la luminance, et α la *force* de l'incrustation.

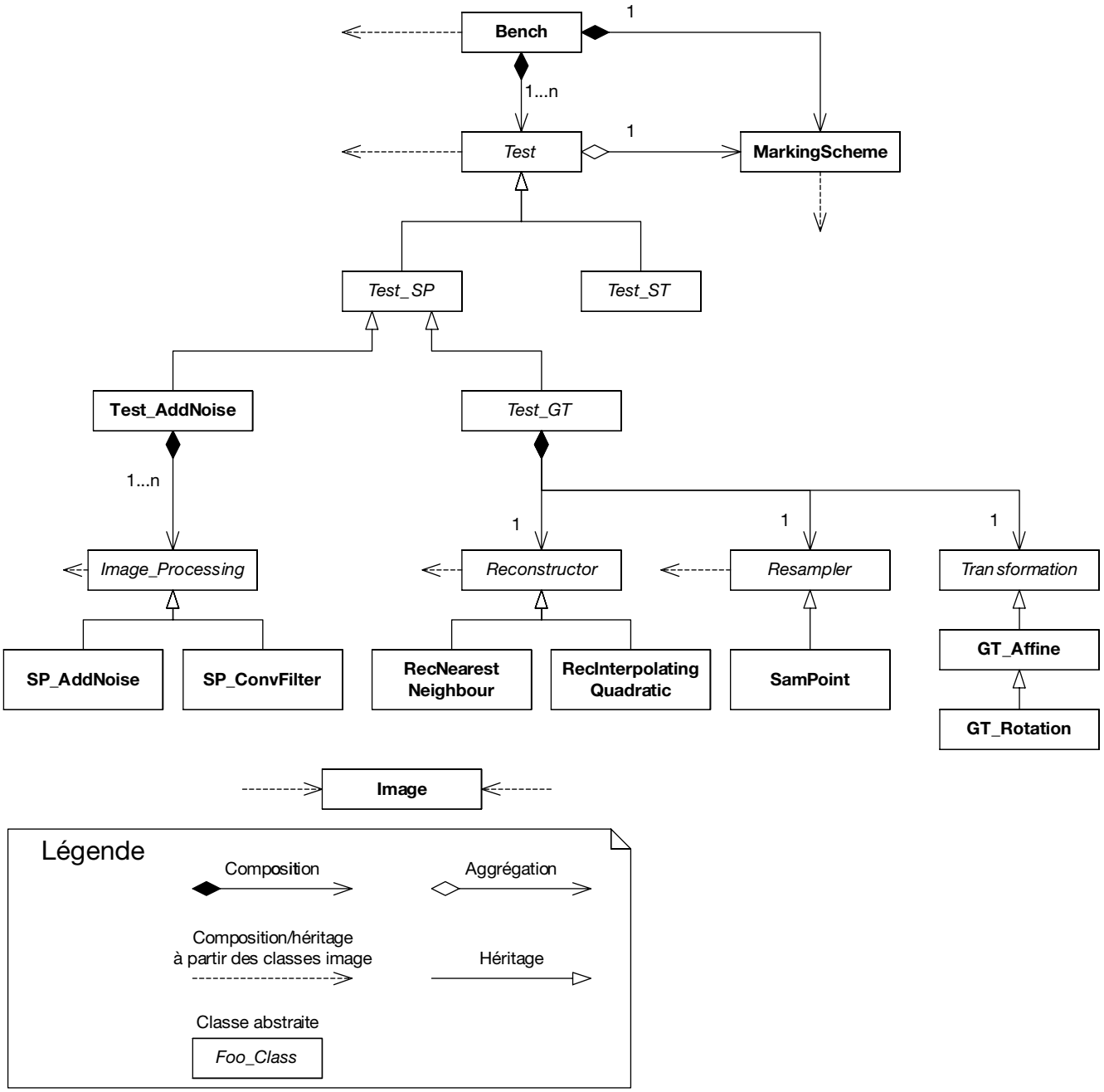

Figure 2. – Schéma UML simplifié de l'arborescence des classes de StirMark Benchmark 4.

`CMedium` gère les données audiovisuelles, et en particulier l'allocation de mémoire. `CTest` prend une liste de média et un schéma de marquage en entrée. Un test correspond à tout ce qui peut être évalué dans une méthode de tatouage, comme le taux de fausses alarmes, le temps d'insertion ou de détection, la robustesse. Enfin, la classe `CMediumTransformation` représente une transformation quelconque applicable à un médium. Par exemple, pour des images, cela comprend des opérations de filtrage, des transformations géométriques. Un `CTest` fait donc couramment appel à une succession de `CMediumTransformation`, bien que ce ne soit pas systématique, comme nous le verrons avec le test pour les faux positifs (voir paragraphe 5.3.).

Bien que les méthodes de tatouage changent en fonction des média, beaucoup de tests demeurent applicables à plusieurs catégories. Ainsi, un test de robustesse se déroule de la manière suivante :

– pour chaque médium dans un ensemble donné

1. dissimuler la marque de sorte que la qualité[2] du médium résultant soit supérieure àun minimum donné ;

2. appliquer une série de transformations sur le médium marqué.

– pour chaque médium marqué et modifié, tenter d'extraire la marque et mesurer le taux d'erreur.

La mesure de robustesse est donnée par la probabilité de détection ou le taux d'erreur sur les bits après extraction. La procédure décrite est paramétrable par un profil. De plus, elle doit être répétée plusieurs fois car un test pourrait réussir par chance ou échouer par malchance. Il apparaît clairement que ce test ne dépend nullement du médium employé : la classe `CMedium` encapsule les média supportés. Cependant, les transformations sous-jacentes doivent, elles, être définies pour chaque type de médium. Par exemple, un filtre Gaussien ne se programme pas de la même manière selon qu'on souhaite l'appliquer à une image ou à un son. Chaque transformation nécessite donc une spécialisation en fonction du médium visé.

L'utilisation d'une structure orientée objet simplifie l'emploi du logiciel. En effet, il est alors très simple de rajouter une nouvelle attaque. Par exemple, dans le cas d'une image, il suffit de dériver `CMediumTransformation` pour décrire comment change la valeur d'un pixel. Il en va de même pour ajouter un test. Les tâches « administratives », comme lire le médium à marquer, appliquer la méthode de tatouage ou sauvegarder les résultats, sont prises en charge par `StirMark Benchmark 4`. Ainsi, un utilisateur n'a qu'à se concentrer sur le code approprié pour les attaques et tests, sans se soucier des problèmes annexes. L'application propose une grande variété de résultats et graphiques, comme ceux introduits dans [KP99].

4. critères d'évaluation

L'évaluation complète d'un schéma de tatouage nécessite de définir précisément, pour chaque caractéristique (imperceptibilité, fiabilité, capacité, rapidité), un niveau d'assurance souhaité. Chaque niveau correspond à un ensemble de contraintes. Pour qu'un niveau soit validé, il faut que la méthode de tatouage les vérifie toutes. Ainsi, des résultats clairs sont fournis en donnant, pour chaque critère, le niveau d'assurance obtenu lors de l'évaluation.

Les niveaux d'assurance s'étalonnent difficilement. Si on en définit trop, l'évaluation devient très complexe et la lisibilité des résultats y perd grandement. Au contraire, peu de niveaux n'offrent pas une granularité suffisante pour différencier les méthodes de tatouage. Les mécanismes d'évaluation des systèmes de sécurité informatique définissent généralement de cinq à sept niveaux. Cette fourchette semble offrir un compromis raisonnable.

4.1. perceptibilité

Le problème est similaire à celui de l'évaluation des algorithmes de compression. Tout comme dans le cas du tatouage, le but est de quantifier les modifications subies par le médium lors d'une transformation. On ne cherche toutefois pas ici à mesurer la perceptibilité de la marque, mais les conséquences de son insertion dans le médium. Cette question (*i.e.* celle de l'évaluation objective *vs.* subjective) est analogue à celle déjà étudiée dans le cadre du codage de source avec pertes (voir [Wat87, JJS93, Com95, KW97]).

Le manque d'une mesure qualitative performante est flagrant. Le PSNR est trop restrictif dans notre cas. Cette mesure ne prend pas en compte le système visuel/auditif humain. Par exemple, pour les images, tous les schémas fondés sur de légères distorsions géométriques, bien souvent imperceptibles à l'œil, seraient automatiquement bannis.

Un niveau d'assurance bas correspondrait à accepter un médium légèrement dégradé, d'un point de vue perceptif. Typiquement, des diffusions audio *via* un réseau présentent déjà ce niveau de qualité. Un niveau moyen rendrait les modifications du médium imperceptibles dans des conditions d'utilisation « grand public ». Le niveau suivant correspond à une amélioration de l'environnement, comme un enregistrement studio pour du son. Enfin, idéalement, la perceptibilité devrait être mesurée à l'aide d'un groupe d'observateurs examinant attentivement le médium marqué dans des conditions très strictes. Ces différents niveaux sont présentés dans le tableau 3.

Tableau 3. – Niveaux d'assurance possibles pour la perceptibilité

Niveau d'assurance	Critères
Bas	– PSNR (lorsqu'applicable) – Légèrement perceptible, mais pas trop gênant
Modéré	– Mesure fondée sur le système visuel humain – Imperceptible dans des conditions normales d'utilisation, *i.e.* grand public
Haut	– Différences imperceptibles lors d'une comparaison avec le médium original dans des conditions type studio
Extrême	– Évaluation par un large panel de personnes dans des conditions strictes

Il apparaît difficile de mettre au point des niveaux d'assurance fiables tant que nous ne disposons pas d'une mesure précise. Les conditions d'utilisations permettent alors d'introduire une distinction, mais l'automatisation du procédé devient délicate.

2. Actuellement, le PSNR est utilisé en guise de mesure. Néanmoins, la modularité de `Stirmark Benchmark 4` permet d'y substituer n'importe quelle autre mesure.

4.2. fiabilité

Deux critères permettent de définir la fiabilité d'un système, la *robustesse* et le taux de *fausses alarmes* (voir 5.3.), dont il existe deux types :
– les *faux positifs* : la détection d'une marque dans un stégomédium est positive alors que celui-ci ne contient pas la marque recherchée (ou pas de marque du tout) ;
– les *faux négatifs* : la détection d'une marque dans un stégomédium échoue alors qu'elle y est bien présente.
Les menaces centrées sur une modification du signal relèvent de la robustesse. Ce terme, selon l'application, revêt des sens différents. Par exemple, dans le cas de la protection des droits d'auteur, il est synonyme de résistance aux attaques qui invalident la marque, soit en la retirant, soit en la rendant illisible. De légères altérations du médium ne doivent pas porter à conséquence. En revanche, lorsqu'il s'agit de vérifier l'intégrité du médium, une autre granularité est recherchée ([WL98, RD00, LC00]). Certaines applications nécessitent la détection immédiate de la moindre modification. D'autres supportent les changements tant que ceux-ci ne dénaturent pas l'interprétation d'un document (*e.g.*, suppression d'un personnage d'une image).
La robustesse peut se mesurer en donnant la probabilité de détection de la marque (ou son taux d'erreur) pour un ensemble de critères appropriés à l'application considérée (*cf.* 3.3.). Ainsi, pour chaque transformation applicable au médium, on en augmente la puissance, en fonction du niveau d'assurance souhaité. Le tableau 4 présente un exemple des conditions minimales à satisfaire afin d'obtenir l'accréditation du niveau considéré. Un schéma qui veut obtenir le niveau « modéré » doit fonctionner pour des images compressées jusqu'à 50 % (en terme de qualité JPEG), ou auxquelles on aura appliqué un filtre médian 3×3.
Le niveau *zéro* ne fournit pratiquement aucune protection supplémentaire. Il correspond aux contraintes imposées par les objectifs de l'algorithme et son environnement. Ainsi, dans le cadre de diffusion radiophonique, cela signifie que la marque résiste à l'émission puis la réception du signal audio.
Le niveau *bas* doit empêcher des utilisateurs « honnêtes » d'altérer la marque dans des conditions normales d'utilisation du médium. L'invalidation de la marque nécessite peu de moyens. Pour des photographies, cela signifie que des opérations de compression, de redimensionnement ou de recadrage de l'image ne retirent pas la preuve de propriété.
Le niveau *modéré* est atteint lorsque des outils plus complexes sont indispensables pour compromettre le schéma. En reprenant l'exemple des photographies, l'emploi d'un outil avancé de traitements d'images ne permettrait pas systématiquement d'altérer la marque.
Le niveau *haut* requiert, en plus d'outils spécifiques, une bonne connaissance et des compétences dans le domaine. Toutes les tentatives pour invalider la marque ne réussissent pas systématiquement, plusieurs tentatives et un peu de travail sur l'approche sont nécessaires.
Le niveau *extrême* implique la mise en œuvre de moyens démesurés, comme des recherches par un groupe de spécialistes, qui rendent le coût de l'attaque bien plus élevé que celui requis pour l'obtention du même médium marqué. Le tableau 4 ne fournit pas de détails sur les valeurs requises car ce niveau correspond à une résistance pratiquement parfaite pour chaque attaque.
La robustesse est *démontrable* lorsqu'il est calculatoirement irréalisable pour un adversaire d'invalider la marque. On peut comparer cela à certains algorithmes de cryptographie fondés sur des problèmes *difficiles* (logarithme discret ou factorisation par exemple).

4.3. capacité

La quantité d'information dissimulable dans le médium résulte souvent d'un compromis entre la robustesse et l'imperceptibilité de la marque. Cette valeur est souvent fixée, plus ou moins arbitrairement.

Tableau 4. – Niveaux d'assurance possibles pour la robustesse

	Niveaux			
	Zéro	Bas	Modéré	Haut
Qualité de compression JPEG	100–90	100–75	100–50	100–25
Réduction de couleurs (GIF)	256	128	64	32
Cadrage	100–90 %	100–75 %	100–50 %	100–25 %
Correction Gamma		0.7–1.2	0.5–1.5	0.3–1.8
Changement d'échelle		1/2–3/2	1/3–2	1/4–4
Rotation		±0–2°	±0–5°, 90°	±0–7°, 180°
Symétrie horizontale		•	•	•
Bruit uniforme		1–5 %	1–15 %	1–25 %
Contraste		±0–10 %	±0–25 %	±0–40 %
Luminosité		±0–10 %	±0–25 %	±0–40 %
Filtre médian			3×3	3×3

Lors de la mise en œuvre d'un schéma de tatouage, il est très utile d'avoir une idée précise de ces compromis. Un graphique faisant varier deux contraintes, la troisième restant constante, est un moyen simple d'y parvenir. Ainsi dans le modèle simple de tatouage à trois paramètres, on peut étudier la relation entre la robustesse et la force de l'attaque lorsque la qualité du médium tatoué est fixée, entre la force de l'attaque et la qualité du médium tatoué, ou encore entre la robustesse et la qualité [KP99].

Le premier graphique est certainement le plus important. Pour une attaque donnée et une qualité de médium après tatouage donnée, il montre le taux d'erreur en fonction de la force de l'attaque. Le deuxième graphique est utile pour l'utilisateur : la performance du système est fixée (par exemple on pourrait imposer qu'au plus 5 % des bits d'information véhiculés soient corrompus afin de pouvoir appliquer des technique de correction d'erreur) et il permet de trouver à quels types d'attaques le système peut résister si l'utilisateur peut s'accommoder de telle ou telle perte de qualité. Ces graphiques seront réalisés automatiquement lors de l'évaluation du schéma.

4.4. rapidité

Notre outil ne traite que l'implantation logicielle des schémas de tatouage. En général, le temps d'exécution n'est pas un critère très fiable de performances[3], sauf si ces exécutions se déroulent toutes dans un environnement identique. Or `StirMark Benchmark 4` offre justement ce cadre. Tous les tests sont entrepris sur une même plate-forme et une seule méthode est évaluée à la fois. Il est évident que cette mesure n'est pertinente que dans un but de comparaison entre les schémas, l'utilisateur final possédant un matériel potentiellement différent de celui employé pour les tests.

5. nouveaux tests

5.1 audio

La précédente version de `StirMark` s'attaquait uniquement des images. Celle-ci s'intéresse également aux fichiers sons. N'importe quelle manipulation d'un fichier audio constitue potentiellement une attaque à l'encontre de la marque dissimulée. En fonction de la manière dont le son est utilisé certaines attaques sont plus probables que d'autres. Nous proposons d'utiliser le type de post-production en studio comme base pour ces attaques. Par exemple, la préparation d'un enregistrement sonore pour une retransmission radiophonique inclus souvent la normalisation et la compression de l'enregistrement, afin d'obtenir un niveau de volume sonore compatible avec la transmission, une équalisation pour optimiser la qualité perçue, un débruiteur et différents filtres permettant de retirer les fréquences nontransmissibles.

Pour rendre possible l'évaluation de méthodes de marquage audio, nous avons constitué des groupes d'attaques. Comme des attaques d'un même groupe reposent sur des principes identiques, il est probable qu'un schéma qui résiste à une attaque donnée dans un groupe résiste également à toutes les autres appartenant à ce même groupe (et inversement si l'algorithme y est vulnérable). Accroître la résistance à une attaque augmente donc la robustesse de la méthode à toutes les attaques du groupe considéré.

Nous avons donc identifié les groupes suivants :

– *dynamique* : porte sur le profil d'amplitude d'un fichier audio. Son augmentation ou sa diminution constitue en soi une attaque. Un limiteur, un expanseur ou un compresseur sont des systèmes plus complexes car ils reposent sur des changements non linéaires dépendant du matériel ;

– *filtrage* : il coupe ou amplifie certaines parties du spectre. Les plus classiques sont les passe-bas et passe-haut, mais les *equalizers* sont aussi assimilables à des filtres ;

– *ambiance* : ces effets simulent la présence d'un endroit (stade, studio, salle de concert, ou autres). Les effets les plus classiques sont la réverbération (*reverb*) et le retard (*delay*), leur paramétrage permettant différentes simulations ;

– *conversion* : le matériel audio est souvent soumis à des changements de format. Par exemple, les sons mono sont dupliqués pour donner du stéréo, la fréquence d'échantillonnage peut passer de 32 kHz à 44 kHz (voire 96 kHz), les conversions numériques/analogiques et analogiques/numériques. Toutes ces conversions impliquent du bruit et des artifices ;

– *compression avec pertes* : ces algorithmes s'appuient sur un modèle psycho-acoustique précis et permettent ainsi de réduire la taille des données d'un facteur 10 ou mieux. Ils s'appuient sur une destruction des informations imperceptibles par un auditeur ;

– *bruit* : la plupart des attaques présentées précédemment introduisent du bruit dans le signal. Les composants matériels dans une chaîne audio injectent eux aussi du bruit dans le signal. Une attaque consiste alors à dégrader le signal en y ajoutant volontairement du bruit ;

– *modulation* : les effets de modulation, comme le vibrato, le chorus, la modulation d'amplitude ou le flanging[4] sont rarement accessibles dans des conditions normales d'utilisation du fichier audio. Cependant, comme la plupart de logiciels les incluent, ils peuvent être utilisés comme attaques ;

– *time stretch* et *pitch shift* : ces opérations changent la durée d'un événement audio, sans en modifier la hauteur, ou bien

3. D'autant plus que le temps d'exécution d'une technologie sous une version logicielle n'est pas forcément un bon indicateur de son potentiel pour une implantation matérielle (si l'application visée le nécessite).

4. Le flanging est créé en mixant un signal avec une copie de lui-même, légèrement « retardé » ; ce retard change constamment.

changent la hauteur en laissant la durée intacte. Ils permettent d'obtenir un accordage précis ou de faire rentrer un signal donné dans une fenêtre temporelle ;

– *permutations d'échantillons* : ce groupe comprend des manipulations qui n'apparaissent jamais dans un environnement usuel. Entre autres, il s'agit de permuter des échantillons, ou d'en abandonner.

Les premiers résultats présentés dans [SPR+01] montrent que les effets d'une attaque dépendent très fortement de la cible. La même attaque est imperceptible sur un morceau alors que ses conséquences sont audibles sur le suivant.

5.2. espace des clés

Considérons un médium marqué à l'aide de la clé k. Le programme de détection/extraction ne doit répondre que ce médium est bien marquéque lorsqu'il utilise cette clé k. Dans tous les autres cas, il doit répondre par la négative. Le nombre total de clés constitue également un facteur important puisqu'un attaquant ne doit pas pouvoir essayer toutes les clés pour déterminer la seule valide. Il est donc vital que l'espace des clés soit de grande taille (au moins 2^{64} éléments). Cela signifie que la clé doit au moins comporter 64 bits sans contrainte (bits d'information). En effet, certaines méthodes fixent des bits, pour des raisons de robustesse, d'imperceptibilité, mais ceux-ci ne doivent alors plus compter dans les degrés de liberté de la clé.

Malheureusement, cela ne suffit pas. En effet, deux clés différentes peuvent produire des interférences entre les marques et fausser ainsi la détection. De ce fait, l'espace des clés est beaucoup plus petit qu'il ne semble. Ainsi, il est important de tester la détection d'une même marque, mais en utilisant des clés différentes pour tenter de relever d'éventuelles interférences. On peut choisir des clés plus ou moins proches de la clé authentique, relativement à la distance de Hamming, pour réaliser ces expériences.

Bœuf et Stern présentent dans [BS01] une faille liée à l'utilisation d'une clé identique pour marquer différents média. L'attaque repose sur une analyse de corrélation de la marque incrustée afin d'en déterminer le profil. Une fois celui-ci connu, il est retiré de chaque médium afin de faire échouer la détection. L'analyse est poursuivie dans [ST01] pour les techniques par étalement de spectre où la nécessité d'employer des clés décorrélées est démontrée.

5.3 fausses alarmes

Deux situations conduisent à une erreur de type *faux positif* :

1. l'algorithme de détection/extraction découvre une marque dans un médium n'en contenant pas ;

2. l'algorithme de détection/extraction découvre une marque m' dans un médium contenant en fait la marque m.

Le premier cas se mesure en considérant un ensemble de média puis en tentant d'y retrouver une même marque. Cette opération doit être répétée plusieurs fois avec des marques différentes.

Pour le second, nous tentons de détecter une marque m' dans le médium tatoué avec m, en utilisant la même clé que celle employée pour dissimuler m. Comme la marque est un mot binaire, nous pouvons tester un nombre significatif de mots binaires situés à une distance donnée de la marque insérée m, en accroissant cette distance au fur et àmesure. Le résultat du test est présenté sous forme d'un vecteur où la composante i représente le taux de faux positifs découverts pour un mot se trouvant à une distance i de m.

5.4. marquage multiple

Il est essentiel de connaître les réactions d'un algorithme à de multiples insertions de marques différentes. Dans une telle situation, soit plusieurs marques sont alors détectables, soit aucune ne l'est ([MB99]). Si de multiples marques sont exploitables, qu'est-ce qui permet de distinguer celle qui est légitime ? Si aucune ne l'est, ceci démontre que la méthode n'est pas assez résistante au tatouage multiple.

Puisque les marques ont des aspects très différents, il est délicat d'estimer l'impact réel de tatouages multiples. En utilisant la distance de Hamming sur l'espace de toutes les marques binaires possibles, étant donnée une marque de référence, on insère, dans le même médium, cette marque de référence et une seconde dont la distance de Hamming à la marque de référence croît. Dans ce type d'attaque, on considère que la première marque est la seule légitime. En effet, cette opération a pour but d'invalider un médium déjà marqué. Il n'est donc pas besoin de permuter l'ordre d'insertion des marques.

6. problèmes ouverts et conclusion

Un problème qui nous préoccupe concerne la soumission du code en elle-même. En effet, un utilisateur peut délibérément envoyer du code malicieux : virus, DoS (Deny of Service), cheval de Troie ou autre. Nous réfléchissons à la structure à donner à notre outil pour limiter les risques liés à ces attaques. Dans la lignée d'une attaque moins directe, nous avons également envisagé le cas d'une personne soumettant une méthode de tatouage au nom d'une autre. Deux situations malveillantes peuvent alors apparaître :

1. la bibliothèque soumise sert s'attribuer l'algorithme d'une autre personne ;

2. la bibliothèque soumise dégrade volontairement ses résultats, afin de nuire à la « réputation » du concepteur initial.

Ces deux points restent encore sans réponse mais la fréquentation attendue (relativement faible) de ce service laisse espérer la possibilité d'un contrôle manuel.

Nous avons décrit dans cet article l'architecture générale de `StirMark Benchmark 4`, un outil d'évaluation automatique pour les algorithmes de tatouage, ainsi qu'un ensemble de nouveaux tests destinés à mesurer les performances de la méthode soumise. Cette évaluation repose sur une librairie fournie par l'utilisateur. Il sélectionne un profil, adaptant ainsi les tests aux objectifs poursuivis par la méthode. Les tests effectués permettent d'attribuer un niveau d'assurance pour chaque critère. Un niveau n'est validé que lorsque toutes les conditions requises pour l'atteindre le sont.

De nombreux tests sont déjà programmés et quelques autres sont encore en gestation. Si l'architecture générale du système automatique d'évaluation est élaborée, sa mise en pratique n'en est encore qu'à ses débuts. Il reste essentiellement deux aspect à améliorer. Tout d'abord, la métrique choisie, le PSNR, ne convient pas à la problématique du tatouage. Elle devra donc être remplacée afin que les tests donnent des informations pertinentes. Enfin, l'autre point à travailler encore concerne la présentation des résultats. Si, comme nous venons de le voir, nous avons précisément défini les mesures à effectuer, nous n'avons rien encore développé.

Nous espérons que cette nouvelle génération d'outil d'évaluation conduira enfin à une analyse fiable et précise des algorithmes de tatouage, de leurs faiblesses et de leurs forces, ainsi qu'à une comparaison pertinente entre les solutions proposées.

BIBLIOGRAPHIE

[BCL+99] J.A. Bloom, I.J. Cox, J.-P.MG. Linnartz, M.L. Miller et C.B.S. Traw, Copy protection for DVD. I*n : Proceedings IEEE*, pp. 1267, juillet 1999.

[Bra98] G.W. Braudaway, Results of attacks on a claimed robust image watermark. *In : Electronic imaging, security and watermarking of multimedia contents*. The Society for Imaging Science and Technology (IS&T) and the International Society for Optical Engineering (SPIE), pp. 122-131, San Jose, California, U.S.A, janvier 1998.

[BS01] J. Bœuf, et J. Stern, An analysis of one of the SDMI candidates. *In : Proceeding of the Information Hiding Workshop*, LNCS, Pittsburg, PA, U.S.A., avril 2001.

[BSC01] X. Bo, L. Shen et W. Chang, Évaluation of the image degradation for a typical watermarking algorithm in the block-dct domain. *In : Proceeding of the Third International Conference on Information and Communications Security (ICICS01)*, Xian, China, novembre 2001.

[Com95] S. Comes, *Les traitements perceptifs d'images numérisées*, Thèse de doctorat, Université catholique de Louvain, Belgium, 1995.

[Eur00] European Broadcasting Union and Union Européenne de Radio Télévision, *Watermarking-call for systems*, mai 2000.

[HSG00] F. Hartung, J.K. Su et B. Girod, Spread spectrum watermarking : Malicious attacks and counterattack. *In : Electronic Imaging, Security and Watermarking of multimedia content II*. The Society of Imaging Science and Technology (IS&T) and the International Society for Optical Engineering (SPIE), pp. 147-158, San Jose, California, U.S.A., janvier 2000. ISSN 0277-786X. ISBN 0-8194-3598-9.

[Int97] International Federation of the Photographic Industry, London, *Request for proposals-embedded signalling systems*, 1997.

[JJS93] N. Jayant, J. Johnston et R. Safranek, Signal compression based on models of human perception. *Proceedings of the IEEE*, vol. 81, n°10, 1993, pp. 1385-1422.

[Kah96] D. Kahn, *The codebrakers*, Scribner, 1996.

[KP99] M. Kutter et F.A.P. Petitcolas, A fair benchmark for image watermarking systems. *In : Electronic imaging, security and watermarking of multimedia content II*, pp. 226-239, San Jose, California, U.S.A., janvier 1999. ISSN 0277-786X. ISBN0-8194-3128-1.

[KVH00] M. Kutter, S. Voloshynovskiy et A. Herrigel, Watermark copy attack. *In : Electronic Imaging, Security and Watermarking of multimedia content II*. Society for Imaging Science and Technology (IS&T) and International Society for Optical Engineering (SPIE), pp. 371-380, San Jose, California, U.S.A., janvier 2000. ISSN 0277-786X. ISBN 0-8194-3598-9.

[KW97] D. Kirby et K. Watanbe, Subjective testing image of mpeg-2 nbc multichannel audio coding. *In : Proceedings of the International Broadcasting Convention (IBC'97)*, pp. 482-487, Amsterdam, Netherlands, septembre 1997.

[LC00] C. Lin et S. Chang, Semi-fragile watermarking for authenticating jpeg visual content. *In : Electronic Imaging, Security and Watermarking of multimedia content II*. The Society for Imaging Science and Technology (IS&T) and the International Society for Optical Engineering (SPIRE), pp. 140-151, San Jose, California, U.S.A., janvier 2000. ISSN 0277-786X. ISBN 0-8194-3598-9.

[LvD98] J.-P.M.G.Linartz, et M. Van Dijk, Analysis of the sensibility attack against electronics watermarks in images. *In : Proceedings of Information Hiding Workshop*, LNCS. pp. 258-272, Portland, Oregon, U.S.A., 1998.

[MB99] F. Mintzer et G.W. Braudaway, If one watermark is good, are more better? *In : International Conference on Acoustics, Speech and Signal Proceeding (ICASSP)*. Institute for Electrical and Electronix Engineers (IEEE), pp. 2067-2070, Phoenix, Arizona, U.S.A., mai 1999.

[MEC98] A.M. Mayache, T. Eude et H. Cherifi, A comparison of image quality models and metrics based on human visual sensitivity. *In : IEEE International Conference on Image Processing*, pp. 409-413, octobre 1998.

[MvOV99] A.J. Menezes, P.C. Van Oorschot et S.A. Vanstone, *Handbook of applied cryptography*, CRC Press, juillet 1999.

[PAK98] F.A.P. Petitcolas, R.J. Anderson et M.G. Khun, Attacks on copyright marking systems. *In : Lecture notes in computer science. Workshop on Information Hiding*, pp. 218-238, Portland, Oregon, U.S.A., avril 1998.

[Pet00] F.A.P. Petitcolas, Watermarking schemes evaluation. *IEEE Signal Processing*, vol. 17 n°5, septembre 2000, pp. 58-64, ISSN 1053-5888.

[PSR+01] F.A.P. Petitcolas, M. Steinebach, F. Raynal, J. Dittman, C. Fontaine, et N. Fatès, A public automated web-based evaluation service for watermarking schemes : Stirmark benchmark. *In : Electronic imaging, security and watermarking of multimedia contents*. Society for Imaging Science and Technology (IS&T) and International Society for Optical Engineering (SPIE), San Jose, California, U.S.A., janvier 2001, ISSN 0277-786X.

[PVM+01] S. Pereira, S. Voloshynovskiy, M. Madueño, S. Marchand-Maillet et T.Pun, second generation benchmarking and application oriented evaluation. *In : Proceedings of Information Hiding Workshop*, LNCS, Pittsburg, PA, U.S.A., avril 2001.

[RD00] C. Rey et J.-L. Dugelay, Blind detection of malicious alterations on still images using robust watermarks. *In : IEE Secure Images and Image Authentication Colloqium*, London, U.K., avril 2000.

[SG00] J.K. Su et B. Girod, Fundamental performance limits of power-spectrum condition-compliant watermarks. *In : Electronic imaging, security and watermarking of multimedia content II*. Society for Optical Engineering (SPIE), pp. 314-325, San Jose, California,U.S.A., janvier 2000. ISSBN 0277-786X. ISBN 0-8194-3598-9.

[SPR+01] M. Steinebach, F.A.P. Petitcolas, F. Raynal, J. Dittman, C. Fontaine, C. Seibel et N. Fatès, Stirmark benchmark : audio watermarking attacks. *In : Multimedia Security. IEEE International Conference on Information Technology : Coding and Computing (ITCC'2001)*, Las Vegas, Nevada, U.S.A., avril 2001.

[ST01] J. Stern et J.-P. Tilich, Automatic detection of a watermarked document using a private key. *In : Proceedings of information Hiding Workshop, LNCS*, Pittsburg, PA, U.S.A., avril 2001.

[VPP+01] S. Voloshynovshiy, S. Pereira, T. Pun, J. Eggers et J. Su, Attacks on digital watermarks : Classification, estimation-based attacks and benchmarks. *IEEE Communications Magazine (Special Issue on Watermarking)*, 2001. – F. Pérez-González, Ed. Invited paper (to appear).

[Wat87] A.B. Watson, Efficiency of an image code based on human vision. *Journal of the Optical Society of America A*, vol. 4, n°12, 1987, pp. 2401-2417.

[WL98] M. Wu et B. Liu, Watermarking for image authentication. *In : Proceedings of the IEEE International Conference on Image Processing (ICIP'98)*, Chicago, Illinois, U.S.A., 1998.

Manuscrit reçu le 18 avril 2001

LES AUTEURS

Frédéric RAYNAL

Frédéric Raynal est en thèse à l'INRIA (Institut National de Recherche en Informatique et Automatique) en France (soutenance prévue en mars 2002). Ses thèmes de recherche comprennent la programmation génétique interactive, l'évaluation des schémas de tatouage et l'étude des liens entre la cryptographie et la dissimulation d'information. Il est aussi très impliqué dans le secteur de la sécurité informatique, en particulier par sa position de rédacteur en chef d'une nouvelle revue consacrée à ce sujet.

Caroline FONTAINE

Caroline Fontaine est Maître de Conférences au LIFL (Laboratoire d'Informatique Fondamentale de Lille), USTL (Université des Sciences et Technologies de Lille) depuis 1999. Elle a soutenu sa thèse en 1998 à l'Université de Paris 6. Ses thèmes de recherche concernent la protection de l'information : cryptographie (principalement autour des systèmes à clé secrète), et tatouage de documents numériques (principalement des images fixes).

Fabien A. P. PETITCOLAS

Fabien A. P. Petitcolas a soutenu sa thèse sur la dissimulation d'information et ses applications en tatouage à l'université de Cambridge. Il travaille actuellement chez Microsoft Research sur les thèmes de la sécurité informatique, l'évaluation des méthodes de tatouage et la stéganographie. Il est l'éditeur du premier livre sur la dissimulation d'information et le tatouage. Il est également impliqué dans de nombreuses conférences dans ces domaines.